Interference Search

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	21	"PUBLIC KEY".CLM. AND "PRIVATE KEY".CLM. AND "DIGITAL SIGNATURE".CLM. AND AUTHENTICAT$3.CLM. AND DATABASE.CLM. AND DECRYPT$3. CLM.	US-PGPUB	OR	OFF	2005/11/09 10:19

updated Search

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	21	"PUBLIC KEY".CLM. AND "PRIVATE KEY".CLM. AND "DIGITAL SIGNATURE".CLM. AND AUTHENTICAT$3.CLM. AND DATABASE.CLM. AND DECRYPT$3.CLM.	US-PGPUB	OR	OFF	2005/11/09 10:23
L2	2258	"PUBLIC KEY" AND "PRIVATE KEY" AND "DIGITAL SIGNATURE" AND AUTHENTICAT$3 AND DATABASE AND DECRYPT$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/09 10:24
L3	998	713/182	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/09 10:24
L4	4442	713/182 OR 713/156 OR 713/175 OR 713/176 OR 380/282 OR 380/285 OR 705/64	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/09 10:25
L5	500	4 AND 2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/09 10:25
L6	89	3 AND 2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/09 10:25

Updated Search

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

"PUBLIC KEY" AND "PRIVATE KEY" AND "DIGITAL SIGNATURE"

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **PUBLIC KEY** AND **PRIVATE KEY** AND **DIGITAL SIGNATURE** AND **AUTHENTICAT$3** AND **DATABASE** AND **DECRYPT$3**

Found **1,171** of **166,357**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Session 8A: Lower bounds on the efficiency of encryption and digital signature schemes

Rosario Gennaro, Yael Gertner, Jonathan Katz

June 2003 **Proceedings of the thirty-fifth annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: pdf(236.93 KB) Additional Information: full citation, abstract, references, index terms

A central focus of modern cryptography is to investigate the weakest possible assumptions under which various cryptographic algorithms exist. Typically, a proof that a "weak" primitive (e.g., a one-way function) implies the existence of a "strong" algorithm (e.g., a private-key encryption scheme) proceeds by giving an explicit construction of the latter from the former. In addition to showing the *existence* of such a construction, an equally important research direction is to explore the < ...

Keywords: black-box, digital signatures, encryption, lower bounds

2 Cryptosystems: Securely combining public-key cryptosystems

Stuart Haber, Benny Pinkas

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Publisher: ACM Press

Full text available: pdf(416.51 KB) Additional Information: full citation, abstract, references, citings, index terms

It is a maxim of sound computer-security practice that a cryptographic key should have only a single use. For example, an RSA key pair should be used only for public-key encryption or only for digital signatures, and not for both.In this paper we show that in many cases, the simultaneous use of related keys for two cryptosystems, e.g. for a public-key encryption system and for a public-key signature system, does not compromise their security. We demonstrate this for a variety of public-key encry ...

3 Password Management and Digital Signatures: Delegation of cryptographic servers for capture-resilient devices

Philip MacKenzie, Michael K. Reiter

November 2001 **Proceedings of the 8th ACM conference on Computer and**

Communications Security
Publisher: ACM Press
Full text available: pdf(312.90 KB) Additional Information: full citation, abstract, references, citings, index terms

A device that performs private key operations (signatures or decryptions), and whose private key operations are protected by a password, can be immunized against offline dictionary attacks in case of capture by forcing the device to confirm a password guess with a designated remote server in order to perform a private key operation. Recent proposals for achieving this allow untrusted servers and require no server initialization per device. In this paper we extend these proposals to enable dynami ...

4 Secret key distribution protocol using public key cryptography
Amit Parnerkar, Dennis Guster, Jayantha Herath
October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

5 Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures
Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(386.51 KB) Additional Information: full citation, abstract, references, index terms

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have explored the practical performance of these proposed constructions in real-world applications, nor have they compared FSS to traditional, non-forward-secure, signatures in a non-asymptotic way.We present an empirical evaluation of several FSS sch ...

Keywords: digital signatures, forward-secure signatures

6 Public key cryptography
Pradosh Kumar Mohapatra
September 2000 **Crossroads**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: html(60.86 KB) Additional Information: full citation, index terms

7 SPV: secure path vector routing for securing BGP
Yih-Chun Hu, Adrian Perrig, Marvin Sirbu
August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4
Publisher: ACM Press

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

8 Some facets of complexity theory and cryptography: A five-lecture tutorial
Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

9 A workload characterization of elliptic curve cryptography methods in embedded environments
I. Branovic, R. Giorgi, E. Martinelli
June 2004 **ACM SIGARCH Computer Architecture News**, Volume 32 Issue 3
Publisher: ACM Press
Full text available: pdf(227.70 KB) Additional Information: full citation, abstract, references

Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key system for constrained environments, because of the small key sizes and computational efficiency, while preserving the same security level as the standard methodsWe have developed a set of benchmarks to compare standard and corresponding elliptic curve public-key methods. An embedded device based on the Intel XScale architecture, which utilizes an ARM processor core was modeled and used for studying the benchmark performan ...

10 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration
Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(107.24 KB) Additional Information: full citation, abstract, references, index terms

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, that is the MS, actually the SIM, the visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS and the UMTS architecture carry the heritage of the GSM's philosophy regarding the user/network authentication and the data ciphe ...

Keywords: PKIs, PLMNs, asymmetric cryptography

11 Constructing fair-exchange protocols for E-commerce via distributed computation of RSA signatures
Jung Min Park, Edwin K. P. Chong, Howard Jay Siegel
July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**
Publisher: ACM Press
Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Applications such as e-commerce payment protocols, electronic contract signing, and certified e-mail delivery require that fair exchange be assured. A fair-exchange protocol allows two parties to exchange items in a fair way so that either each party gets the other's item, or neither party does. We describe a novel method of constructing very efficient fair-exchange protocols by distributing the computation of RSA signatures. Specifically, we employ multisignatures based on the RSA-signature sch ...

Keywords: Fair-exchange protocols, RSA signatures, e-commerce, multisignatures, zero-knowledge proofs

12 The digital signature standard
CORPORATE NIST
July 1992 **Communications of the ACM**, Volume 35 Issue 7
Publisher: ACM Press
Full text available: pdf(3.12 MB) Additional Information: full citation, references, citings, index terms

13 An authorization model for a public key management service
Pierangela Samarati, Michael K. Reiter, Sushil Jajodia
November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4
Publisher: ACM Press
Full text available: pdf(337.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Public key management has received considerable attention from both the research and commercial communities as a useful primitive for secure electronic commerce and secure communication. While the mechanics of certifying and revoking public keys and escrowing and recovering private keys have been widely explored, less attention has been paid to access control frameworks for regulating access to stored keys by different parties. In this article we propose such a framework for a key management ser ...

Keywords: Access control, authorizations specification and enforcement, public key infrastructure

14 Fine-grained control of security capabilities
Dan Boneh, Xuhua Ding, Gene Tsudik
February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1
Publisher: ACM Press
Full text available: pdf(128.09 KB) Additional Information: full citation, abstract, references, index terms

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

Keywords: Certificate Revocation, Digital Signatures, Public Key Infrastructure

15 Efficient verifiable encryption (and fair exchange) of digital signatures
Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

16 Verifiable encryption of digital signatures and applications
Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(256.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

17 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure
Albert Levi, M. Ufuk Caglayan, Cetin K. Koc
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

18 Encryption and Secure Computer Networks
Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

19 Digital signatures with RSA and other public-key cryptosystems
Dorothy E. Denning
April 1984 **Communications of the ACM**, Volume 27 Issue 4
Publisher: ACM Press
Full text available: pdf(374.39 KB) Additional Information: full citation, references, citings, index terms

Keywords: cryptanalysis, cryptographic, hashing, homomorphism, protocol

20 Who's got the key?
David Henry
November 1999 **Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations**
Publisher: ACM Press
Full text available: pdf(30.32 KB) Additional Information: full citation, references, index terms

Keywords: PKI, certificate authority, encryption

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next